Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1, 2, 4, 7-9, 12 and 14-30 are pending in the application, with 1, 21, and 22 being the independent claims. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 103

Hobson in view of Fischer in view of Peleg in view of Shacham

Claims 1, 2, 4, 9, 12, and 14-30 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over U.S. Patent No. 6,209,016 to Hobson et al. (hereafter "Hobson") in view of U.S. Patent No. 6,237,016 to Fischer et al. (hereafter "Fischer") in view of U.S. Patent No. 6,385,634 to Peleg et al. (hereafter "Peleg") in view of U.S. Patent Publication 2002/0039420 to Shacham et al. (hereafter "Shacham"). Applicants respectfully traverse the rejection and provide the following arguments to support patentability.

Claim 1, as amended, recites a server to perform computations to establish a secure network session. The server includes the features of:

> a system memory; and
>
> a processing unit coupled to said system memory via a system bus, said processing unit obtains values for a modulus N, a private key d, and a cipher text C sent by a client and calculates a value for clear text M for

each request for a secure network session made to said server by said client, said processing unit includes:

> an execution unit, coupled to a decode unit, configured to execute arithmetic instructions to perform product and square operations, said execution unit including at least two multipliers connected directly with said system memory for multiplying data provided from said system memory, and at least one adder connected directly with said at least two multipliers for applying an addition operation to outputs of said at least two multipliers, said execution unit configurable to perform specified multiplication operations in parallel and configurable to perform specified multiplication and addition operations in parallel;
>
> said decode unit to receive requests for establishing a secure network session from said client, said decode unit configured to determine if a square operation or a product operation needs to be performed on an operand, said decode unit further configured to issue said arithmetic instructions to said execution unit so that said execution unit performs specified multiplication and addition operations in parallel and performs specified multiplication operations in parallel while performing either said square or product operation.

(*see*, claim 1, as amended).

Applicants respectfully submit that the claim 1 as amended is patentable over the art of record. For example, as will be discussed below, Hobson does not teach nor suggest at least the feature of "[the] execution unit including at least two multipliers connected directly with [the] system memory for multiplying data provided from [the] system memory, and at least one adder connected directly with [the] at least two multipliers for applying an addition operation to outputs of [the] at least two multipliers" as recited by claim 1.

As shown in FIG. 2 of its accompanying description, the multipliers included within the co-processor of Hobson are not directly connected to the memory and/or the adders of Hobson. For example, a multiplexer Mx3 is coupled between a multiplier

MUL1 and an adder ADD1. As a result, Hobson does not teach nor suggest at least the feature of "[the] execution unit including at least two multipliers connected directly with [the] system memory for multiplying data provided from [the] system memory, and at least one adder connected directly with [the] at least two multipliers for applying an addition operation to outputs of [the] at least two multipliers" as recited by claim 1. The combination of Fischer, Peleg, and Shacham does not provide the missing teaching or suggestion with respect to claim 1. Accordingly, the combination Hobson, Fischer, Peleg, and Shacham cannot render obvious independent claim 1. Dependent claims 2, 4, 9, 12, 14-20, and 23-30 are likewise not rendered obvious by the combination Hobson, Fischer, Peleg, and Shacham for the same reasons as the independent claim from which they respectively depend and further in view of their own respective features. Accordingly, Applicants respectfully request that the rejection of claims 1, 2, 4, 9, 12, 14-20, and 23-30 under 35 U.S.C. § 103(a) be reconsidered and withdrawn.

Claim 21[1] recites a method to establish a secure network session. The method includes the steps of:

> sending an encrypted message to a server using a public key;
>
> decrypting said encrypted message by said server using a private key; and
>
> generating a symmetrical key to encrypt/decrypt messages transmitted and received between a client and said server, wherein generation of said public key, said private key, and/or said symmetrical key further comprises computation of a modular exponentiation operation using a Montgomery method, wherein said Montgomery method further comprises:
>
> > receiving, by a decode unit, a request to perform a modular operation;

[1] Applicants have amended claim 21 solely to correct for a minor informality

> determining, by said decode unit, whether a Montgomery square operation or a Montgomery product operation is to be performed;
>
> issuing, by said decode unit, a first instruction to perform a Montgomery square operation;
>
> issuing, by said decode unit, a second instruction to perform a Montgomery product operation;
>
> performing, by an execution unit, simultaneous multiplication operations in response to at least one of said first instruction and said second instruction; and
>
> performing, by said execution unit, simultaneous multiplication and addition operations in response to at least one of said first instruction and said second instruction.
>
> (*see*, claim 21).

The Office Action dated March 23, 2007 (herein "Office Action"), states that Hobson does not teach or suggest at least the features of "issuing, by [the] decode unit, a first instruction to perform a Montgomery square operation" and/or "issuing, by [the] decode unit, a second instruction to perform a Montgomery product operation" as recited by claim 21. (*see*, Office Action, Page 10 through Page 11). For the reasons to be discussed below in conjunction with claim 22, Fischer does not provide this missing teaching or suggestion with respect to claim 21. Accordingly, the combination of Hobson, Fischer, Peleg, and Shacham does not render obvious independent claim 21. Accordingly, Applicants respectfully request that the rejection of claim 21 under 35 U.S.C. § 103(a) be reconsidered and withdrawn.

Claim 22[2] recites a method to establish a secure network session. The method includes the steps of:

> sending an encrypted message to a server using a public key;

[2] Applicants have amended claim 22 solely to correct for a minor informality

decrypting said encrypted message by said server using a private key; and

generating a symmetrical key to encrypt/decrypt messages transmitted and received between a client and said server, wherein said public key, said private key, and/or said symmetrical key further comprises computation of a modular exponentiation operation using a Montgomery method, wherein said Montgomery method further comprises:

determining, by a decode unit, whether to perform a Montgomery square operation or a Montgomery product operation;

issuing, by said decode unit, a first set of instructions for an execution unit to perform said Montgomery square operation, said first set of instructions comprising:

a first instruction to perform simultaneous multiplication operations; and

a second instruction to perform simultaneous multiplication and addition operations; and

issuing, by said decode unit, a second set of instructions for said execution unit to perform said Montgomery product operation, said second set of instructions comprising:

a third instruction to perform simultaneous multiplication operations;

a fourth instruction to perform simultaneous multiplication and addition operations; and

a fifth instruction to perform simultaneous multiplication and addition operations.

(see, claim 22).

The Office Action dated March 23, 2007 (herein "Office Action"), states that Hobson does not teach or suggest at least the steps of "issuing, by [the] decode unit, a first set of instructions for an execution unit to perform [the] Montgomery square operation, [the] first set of instructions comprising: a first instruction to perform simultaneous multiplication operations; and a second instruction to perform simultaneous

multiplication and addition operations" and/or "issuing, by [the] decode unit, a second set of instructions for [the] execution unit to perform [the] Montgomery product operation, [the] second set of instructions comprising: a third instruction to perform simultaneous multiplication operations; a fourth instruction to perform simultaneous multiplication and addition operations; and a fifth instruction to perform simultaneous multiplication and addition operations" as recited by claim 22. (*see*, Office Action, Page 14 through Page 15). The Office Action alleges that the accompanying description of Fischer's FIG. 2A, namely col. 8, lines 12-41, disclose a "first instruction to perform simultaneous multiplication operations and [a] second instruction to perform simultaneous multiplication-addition operations." (*see*, Office Action, Page 14). The most relevant portion of Fischer provides,

> the multiply-add instruction multiplies together corresponding data elements of the first and second operands generating four intermediate results (e.g., A_3 B_3, A_2 B_2, A_1 B_1, and A_0 B_0). These intermediate results are summed by pairs producing two results (e.g., A_3 B_3 $+A_2$ B_2 and A_1 B_1 $+A_0$ B_0) that are packed into their respective elements of a result 230. Thus, the result 230 is packed data item including a first data element storing A_3 B_3 $+A_2$ B_2 and a second data element storing A_1 B_1 $+A_0$ B_0. Thus, the described embodiment of the multiply-add instruction performs, in parallel, two "multiply-add operations".
>
> (see, Fischer, col. 8, lines 22- 32).

The above cited text of Fischer merely discloses a "multiply-add instruction." Nowhere does Fischer teach or suggest a separate distinct instruction to perform simultaneous

multiplication operations as recited by claim 22. In fact, the disclosure of Fischer does not teach or suggest that the multiplication portion may be performed separately and distinct from the multiply-add instruction. Additionally, as shown in FIG. 1 of Fischer, the instructions set for the computer system of Fischer does not include a multiplication instruction. Therefore, Fischer does not teach or suggest a "first instruction to perform simultaneous multiplication operations and [a] second instruction to perform simultaneous multiplication-addition operations" as alleged in the Office Action. (*see*, Office Action, Page 14). As a result, Fischer does not teach or suggest "issuing, by [the] decode unit, a first set of instructions for an execution unit to perform [the] Montgomery square operation, [the] first set of instructions comprising: a first instruction to perform simultaneous multiplication operations; and a second instruction to perform simultaneous multiplication and addition operations" and/or "issuing, by [the] decode unit, a second set of instructions for [the] execution unit to perform [the] Montgomery product operation, [the] second set of instructions comprising: a third instruction to perform simultaneous multiplication operations; a fourth instruction to perform simultaneous multiplication and addition operations; and a fifth instruction to perform simultaneous multiplication and addition operations" as recited by claim 22. Accordingly, the combination of Hobson, Fischer, Peleg, and Shacham does not render obvious independent claim 22. Accordingly, Applicants respectfully request that the rejection of claim 22 under 35 U.S.C. § 103(a) be reconsidered and withdrawn.

Hobson in view of Fischer in view of Peleg in view of Shacham and in further view of Curiger

Claims 7 and 8 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hobson in view of Fischer in view of Peleg in view of Shacham and in further view of U.S. Patent No. 6,064,740 to Curiger et al. (herein "Curiger").

For reasons discussed above in regard to claim 1, the combination of Hobson, Fischer, Peleg, and Shacham does not render obvious independent claim 1. Curiger does not provide the missing teaching or suggestion with respect to independent claim 1. Accordingly, the combination of Hobson, Fischer, Peleg, Shacham, and Curiger cannot render obvious independent claim 1. Dependent claims 7-8 are likewise not rendered obvious by the combination of Hobson, Fischer, Peleg, Shacham, and Curiger for the same reasons as independent claim 1 from which they respectively depend and further in view of their own respective features. Accordingly, Applicant respectfully requests that the rejection of claims 7 and 8 under 35 U.S.C. § 103(a) be reconsidered and withdrawn.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Jeff H Lewis (44,757)

for Robert Sokohl
Attorney for Applicants
Registration No. 36,013

Date: 9/21/07

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600
700623_4.DOC